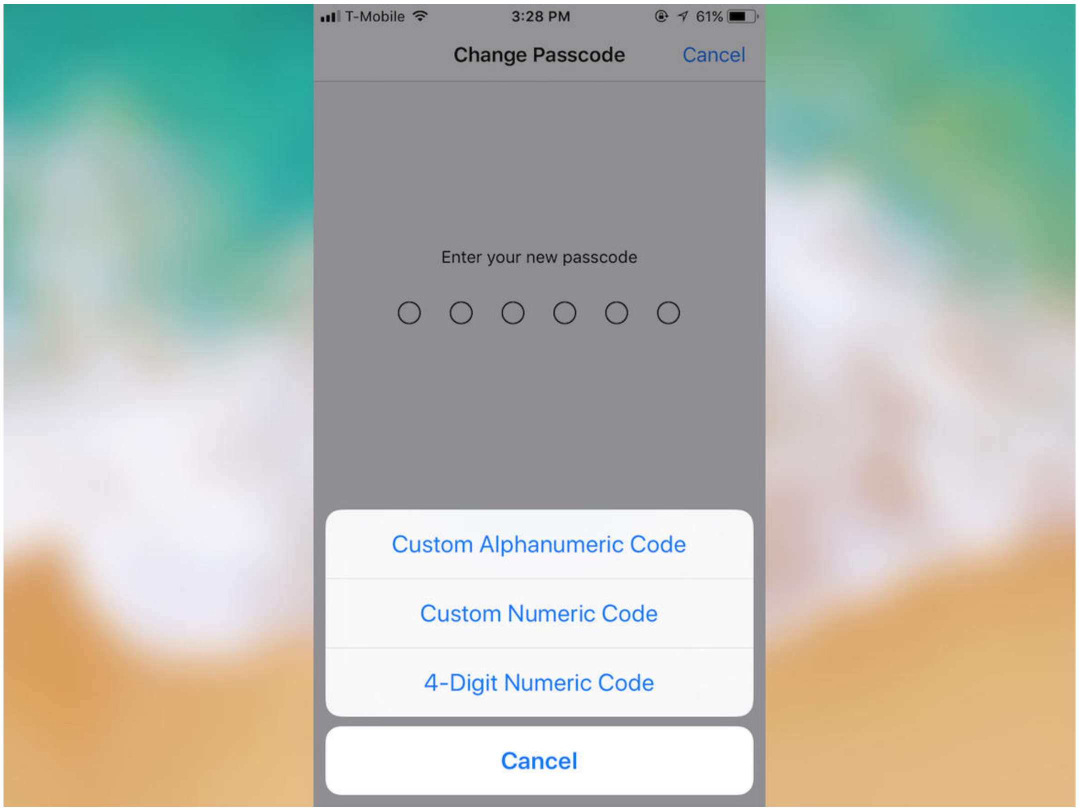
New to iOS 11? Change these privacy and security settings right now

Before you do anything on your iPhone or iPad, you should lock it down. This is how you do it.

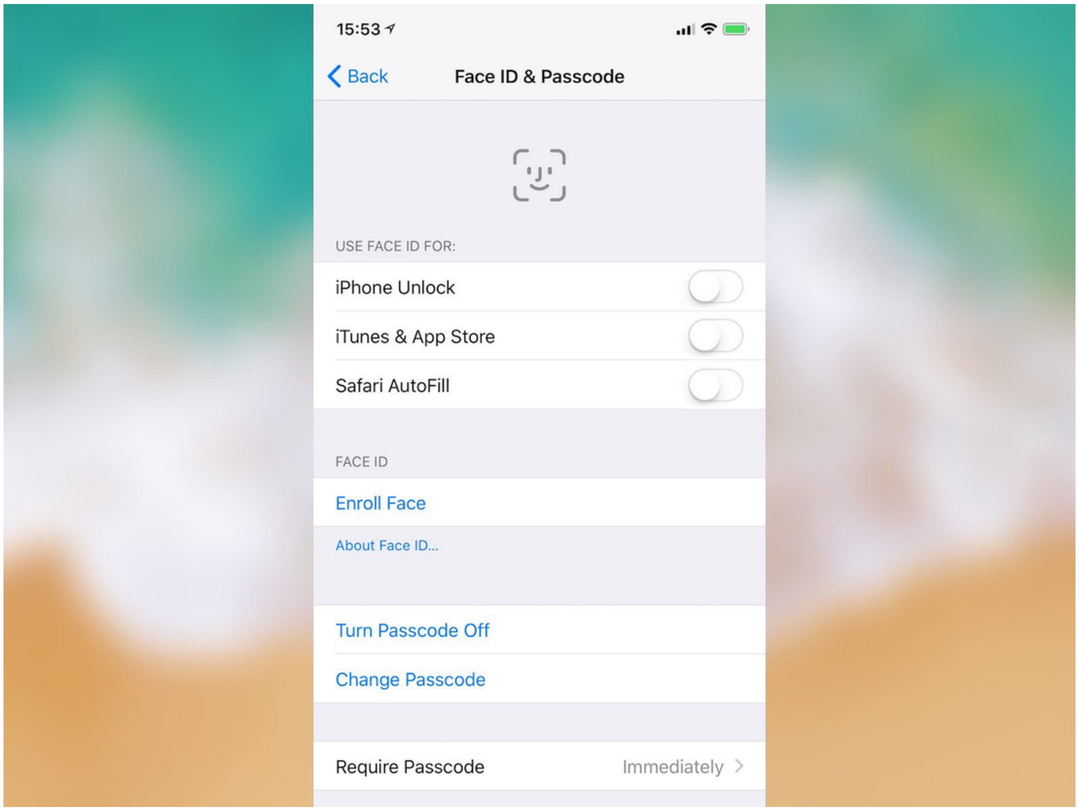
These are the most important privacy settings in iOS 11

New to iOS 11? The first thing you should do is take note of these privacy and security steps to lock down your device.



Set a strong six-digit (or longer) passcode

Data on your iPhone or iPad is encrypted with a passcode.
Go to **Settings > Touch ID & Passcode**, and enter your existing passcode if you have one. If not, select **Turn Passcode On**, and then select **Passcode Options**. This gives you the option of a custom alphanumeric or numeric code, or the older four-digit numeric code.



15:53

Back | Face ID & Passcode

USE FACE ID FOR:

iPhone Unlock

iTunes & App Store

Safari AutoFill

FACE ID

Enroll Face

About Face ID...

Turn Passcode Off

Change Passcode

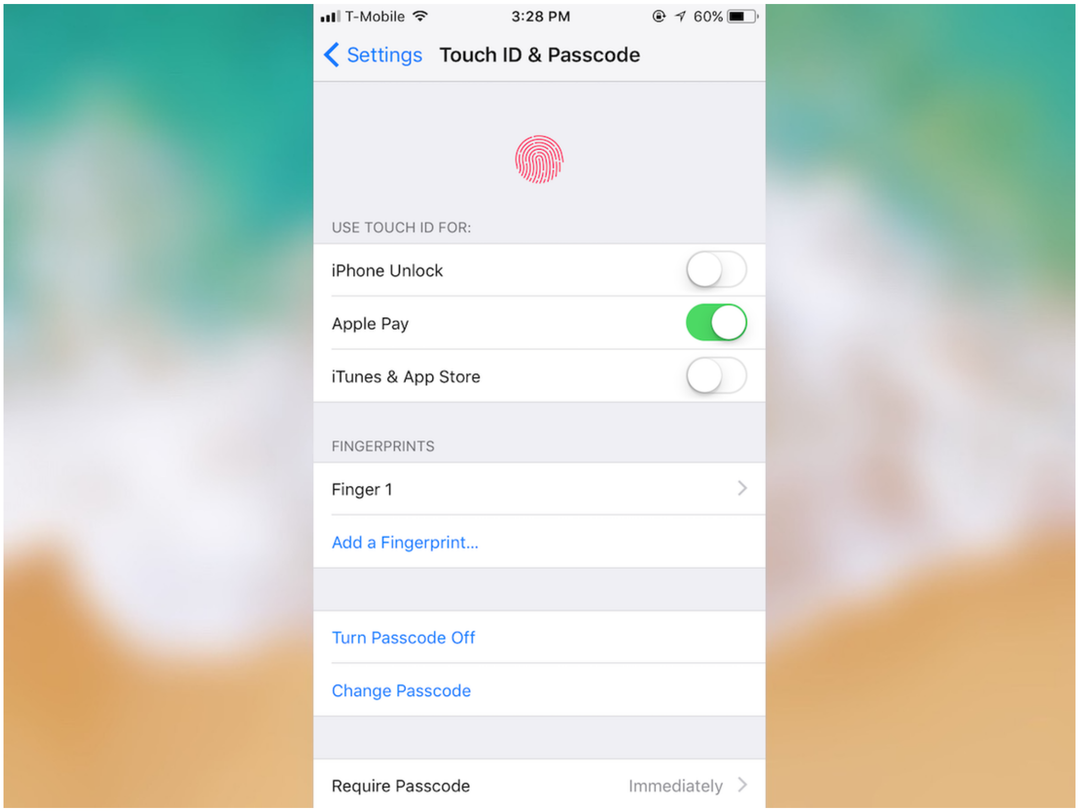
Require Passcode | Immediately

Face ID (iPhone X only)

Face ID is the new way on the iPhone X to unlock your phone. This powerful biometric sensor uses a infrared camera, and this is backed up by a dot projector that is used to bean an array of 30,000 invisible dots at the user's face that are used to create a detailed 3D model of the face being captured.

But biometrics can be used against you. Police in the US have compelled suspects to unlock their phones with fingerprints and facial recognition is no different.

Go to **Settings** > **Face ID & Passcode**, then enter your passcode. You can enrol you face from here if you choose to use it.



USE TOUCH ID FOR:

iPhone Unlock ○

Apple Pay ●

iTunes & App Store ○

FINGERPRINTS

Finger 1 >

Add a Fingerprint...

Turn Passcode Off

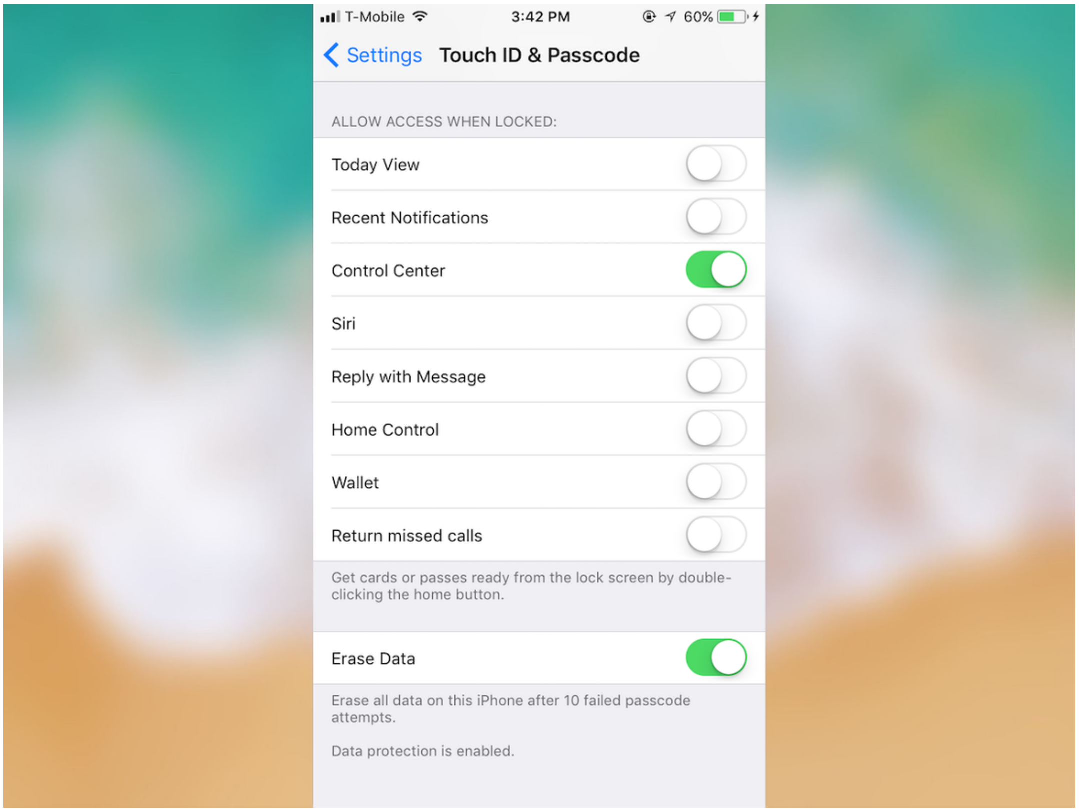
Change Passcode

Require Passcode Immediately >

Turn off fingerprint unlocking

Fingerprints and thumbprints might be convenient, but they can be used against you.

Go to **Settings > Touch ID & Passcode,** then enter your passcode. Make sure the **Phone Unlock** setting is disabled.



T-Mobile 3:42 PM 60%

Settings Touch ID & Passcode

ALLOW ACCESS WHEN LOCKED:

Today View ☐

Recent Notifications ☐

Control Center ☑

Siri ☐

Reply with Message ☐

Home Control ☐

Wallet ☐

Return missed calls ☐

Get cards or passes ready from the lock screen by double-clicking the home button.

Erase Data ☑

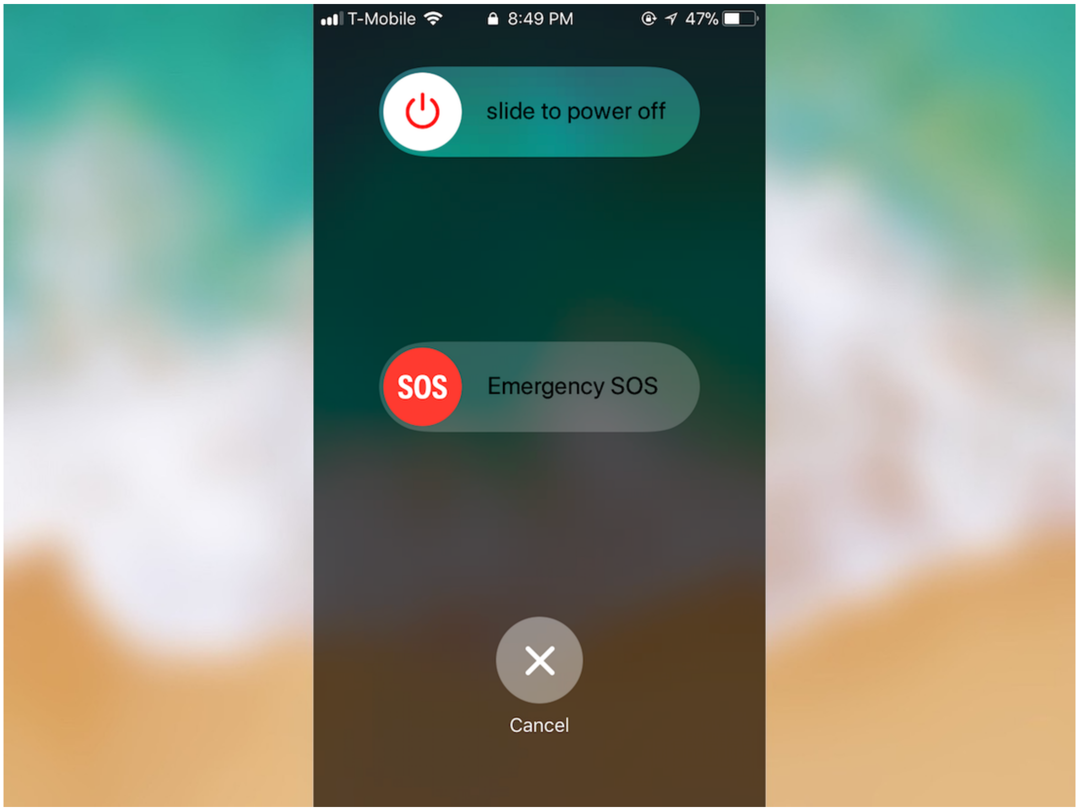
Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

Switch off Home screen features

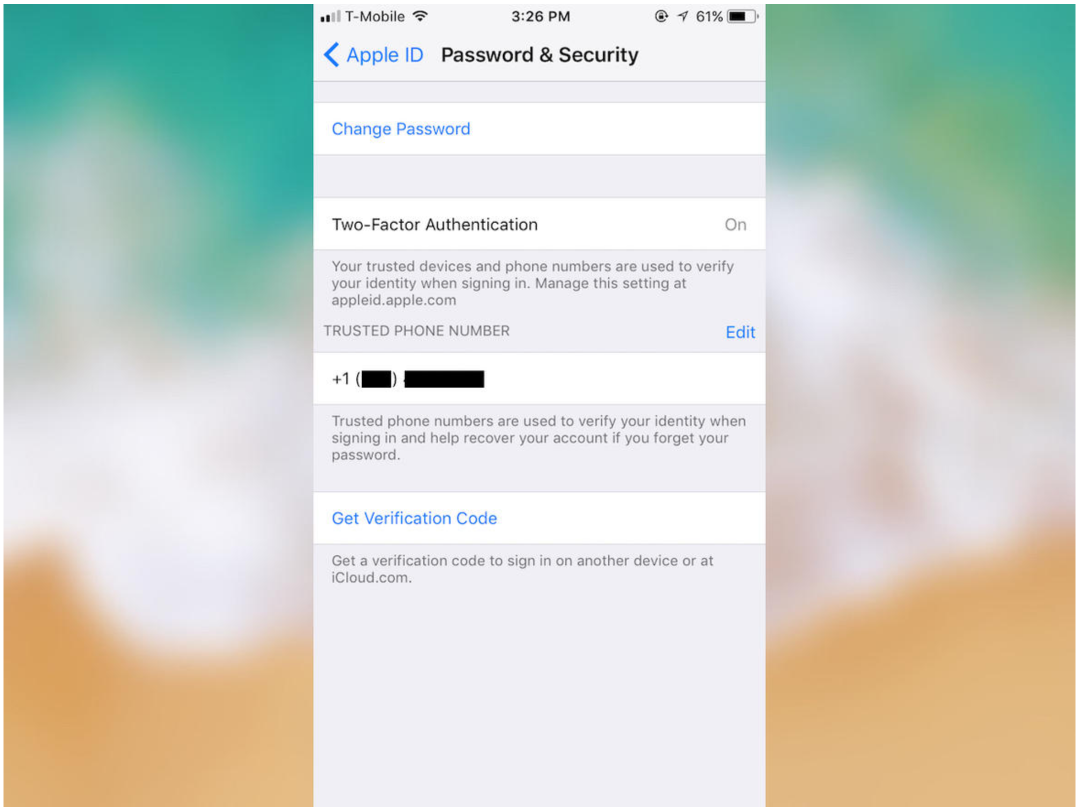
Don't give away free access to your locked iPhone through things like Siri.

Go to **Settings > Touch ID & Passcode**, and enter your passcode. Scroll down to see your lock screen access. The fewer items that are on, the better. From here, you can turn off your Today view, your wallet access, and other features, like Siri and Home Control -- and now Return Missed Calls, a new feature of iOS 11.



Shut off biometrics

iOS 11 now lets you force-activate the passcode instead of using Face ID or Touch ID. That's a good thing if you're in a panic situation or want to protect your data -- just push the power button five times or squeeze your iPhone X. You cannot be legally compelled to unlock a device with a just a passcode under the Fifth Amendment, which protects what's stored in your head, but not what's on your body.



T-Mobile 3:26 PM 61%

Apple ID Password & Security

Change Password

Two-Factor Authentication On

Your trusted devices and phone numbers are used to verify your identity when signing in. Manage this setting at appleid.apple.com

TRUSTED PHONE NUMBER Edit

+1 ([redacted]) [redacted]

Trusted phone numbers are used to verify your identity when signing in and help recover your account if you forget your password.

Get Verification Code

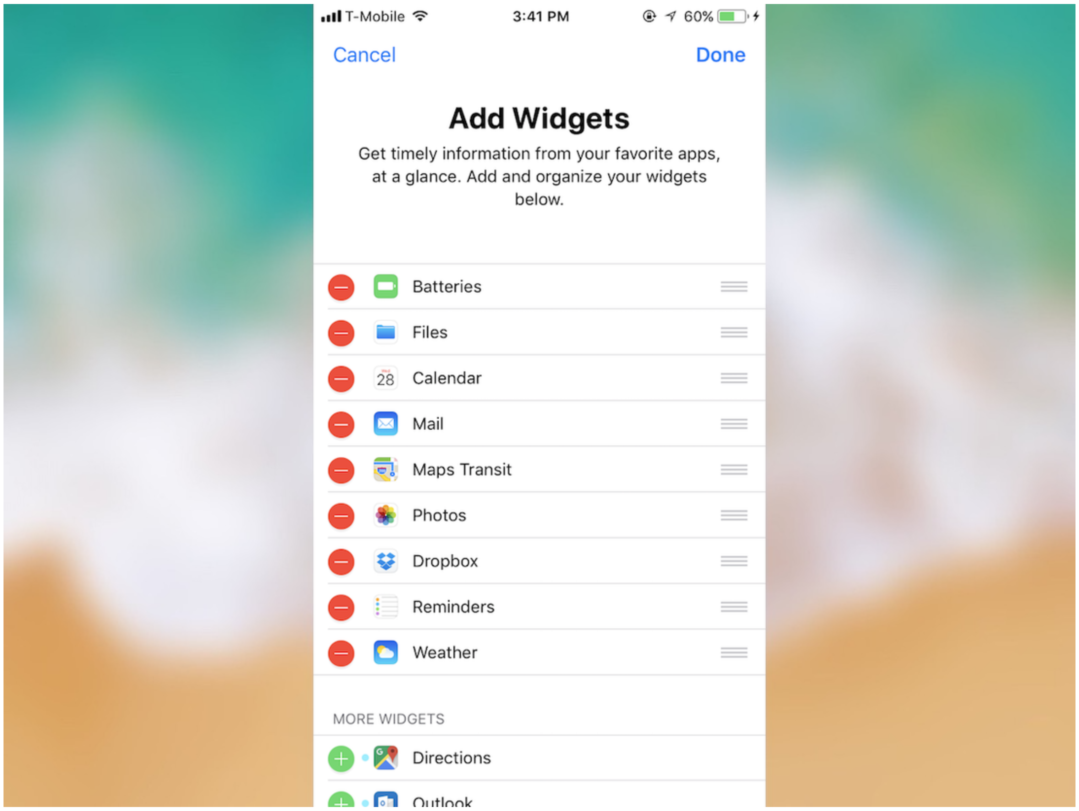
Get a verification code to sign in on another device or at iCloud.com.

Set up two-factor authentication

Two-factor authentication is one of the best ways to stop hackers from accessing your data. Before Apple lets you into your account, it sends a code to a device that only you will own, which prevents someone from taking your data even with your username and password.

Go to **Settings** > and tap your name at the top, then go to **Password & Security**, then **Two-Factor Authentication**.

Setting up two-factor authentication takes just a few minutes. Our sister site CNET has a helpful guide on how to do it.



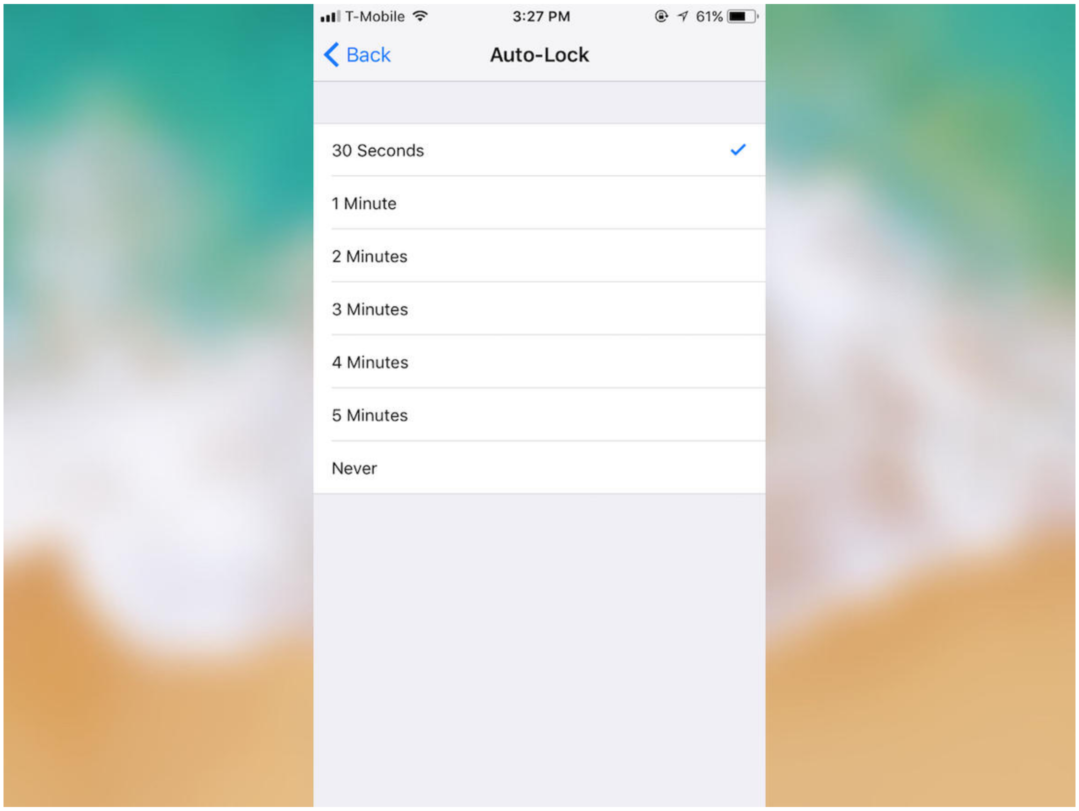
Add Widgets

Get timely information from your favorite apps, at a glance. Add and organize your widgets below.

Switch off data-leaking widgets

Gone are the days when your iPhone acted as a security checkpoint. Swipe-right on your phone opens up Today View, which lets you see at a glance from your lock screen your events for the day, news, and in some cases personal information.

You can turn off each panel by **swiping to the right on the Home screen** (into the Today View pane), then scrolling to the bottom, and selecting **Edit**. From there, you can remove each panel as necessary.



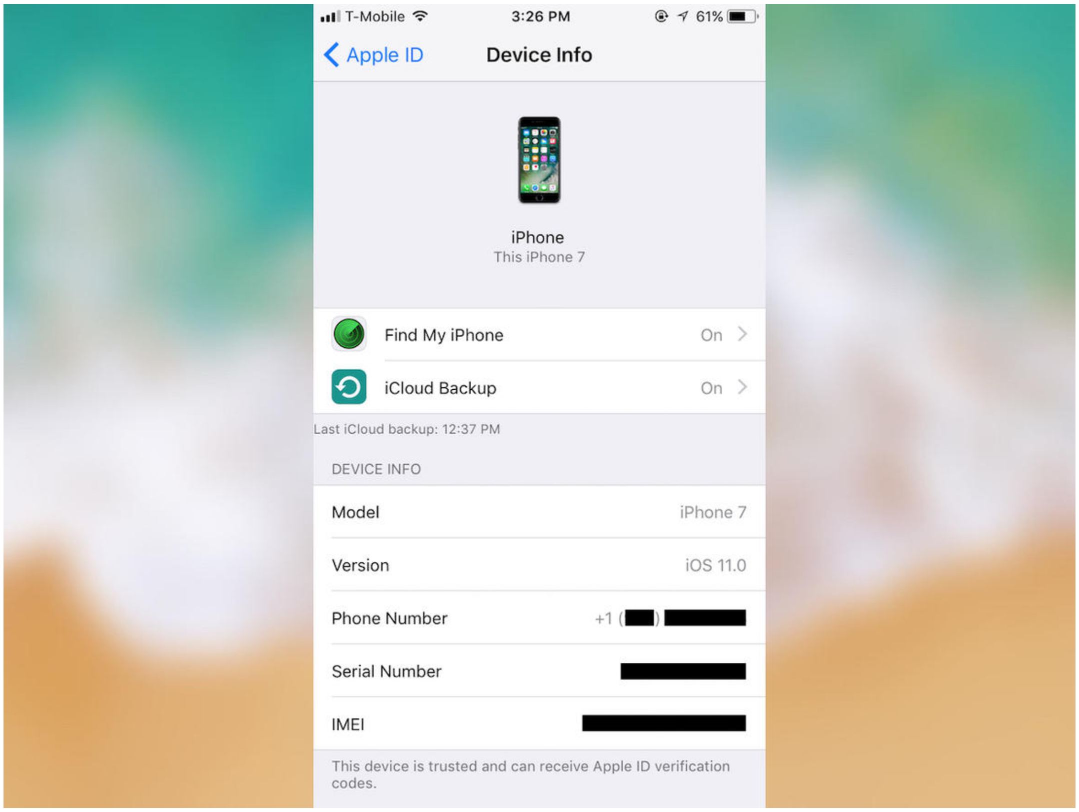
Auto-Lock

- 30 Seconds ✓
- 1 Minute
- 2 Minutes
- 3 Minutes
- 4 Minutes
- 5 Minutes
- Never

Reduce your lock screen timeout

The shorter the lock screen setting, the faster your iPhone or iPad display will shut off before anybody can get access to it.

You can lower the auto-lock period by going to **Settings** > **Display & Brightness** > **Auto-Lock**. The lower the number, the better.



T-Mobile 3:26 PM 61%

< Apple ID Device Info

iPhone
This iPhone 7

Find My iPhone	On >
iCloud Backup	On >

Last iCloud backup: 12:37 PM

DEVICE INFO

Model	iPhone 7
Version	iOS 11.0
Phone Number	+1 ([redacted]) [redacted]
Serial Number	[redacted]
IMEI	[redacted]

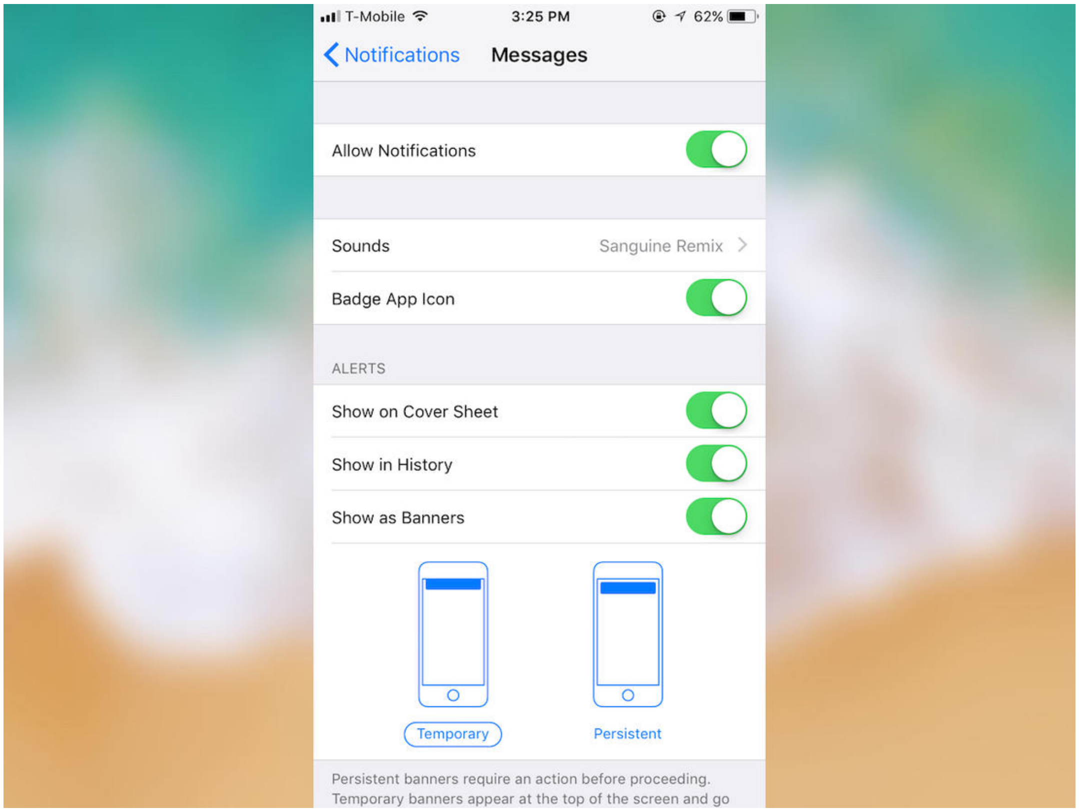
This device is trusted and can receive Apple ID verification codes.

Switch on "Find My iPhone"

Apple's Find My iPhone tells you where your device is if you mark it lost or stolen.

Head to **Settings,** then tap your name at the top, then go to **iCloud**, then **Find My iPhone,** (or iPad) and make sure that it is switched on. You may need to enter your device passcode to authorize this.

Also, by selecting **Send Last Location**, with the last few percent of battery life, your device will update Apple's servers with its last location -- just before it powers down.



T-Mobile 3:25 PM 62%

< Notifications Messages

Allow Notifications

Sounds Sanguine Remix >

Badge App Icon

ALERTS

Show on Cover Sheet

Show in History

Show as Banners

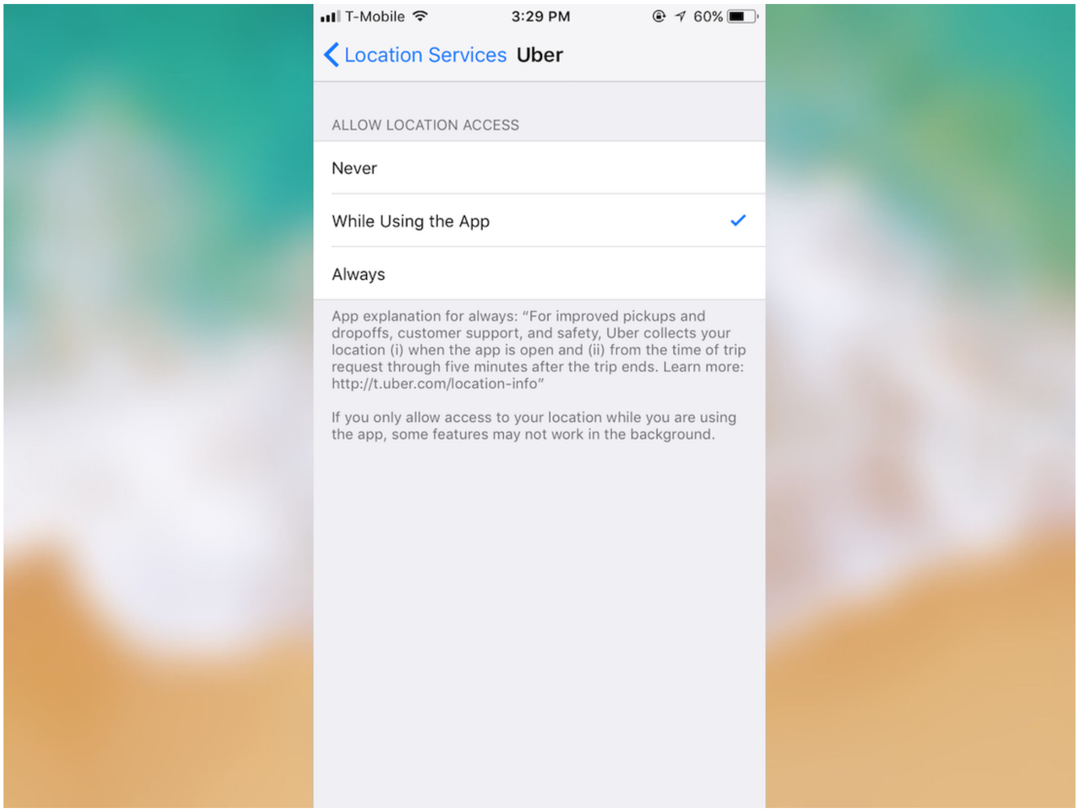
Persistent banners require an action before proceeding.
Temporary banners appear at the top of the screen and go

Tame your notifications

iOS 11, like other versions of the software, show previews of your messages and emails on your lock screen, allowing anyone with access to your iPhone or iPad to take a glimpse.

To limit this feature, for example, to just showing the sender of the message, go to **Settings > Notifications** and then select **Messages** and **Mail** for text messages and iMessages and email, respectively. From each screen, you can change the preview style. For maximum privacy, disable **Show Previews** so messages won't be displayed on the lock screen.

A new feature, dubbed Persistent Banners, will alert you but require action before moving on.



ALLOW LOCATION ACCESS

Never

While Using the App ✓

Always

App explanation for always: "For improved pickups and dropoffs, customer support, and safety, Uber collects your location (i) when the app is open and (ii) from the time of trip request through five minutes after the trip ends. Learn more: http://t.uber.com/location-info"

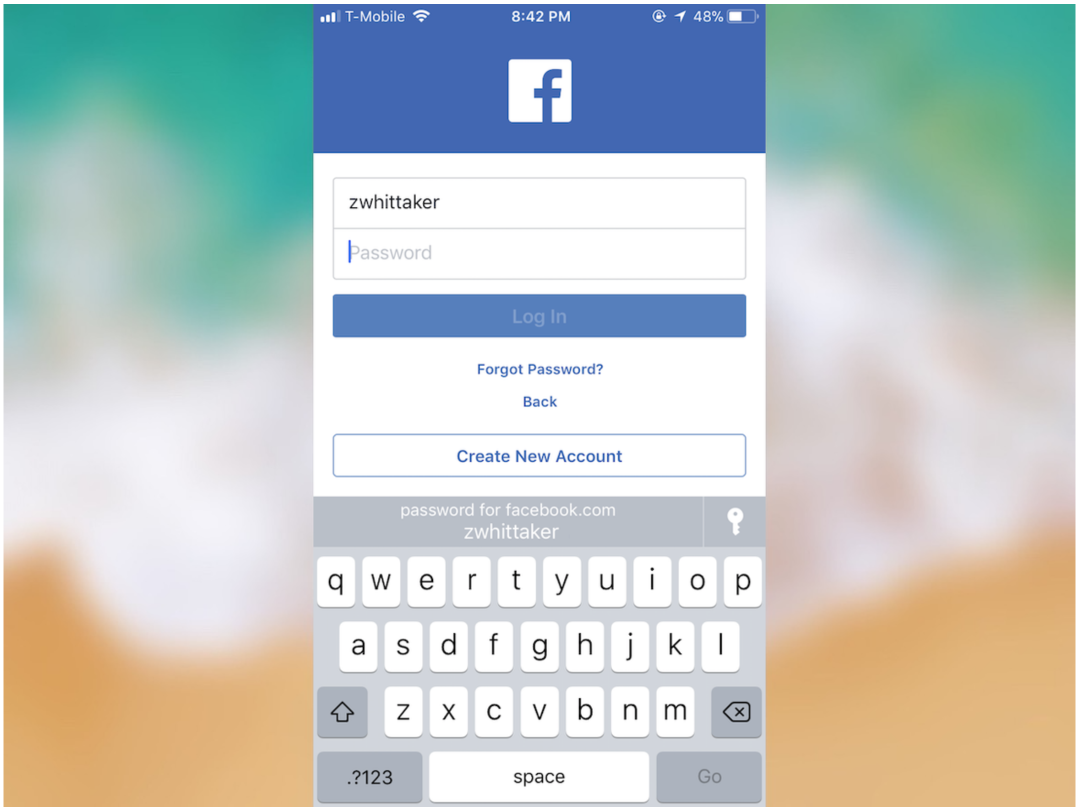
If you only allow access to your location while you are using the app, some features may not work in the background.

Reset your app location settings

Your apps can take a lot of liberties -- especially when it comes to your data. Some apps, like Uber, sparked controversy when they used user location at all times rather than only while they were using the app. And there was no way to turn it off.

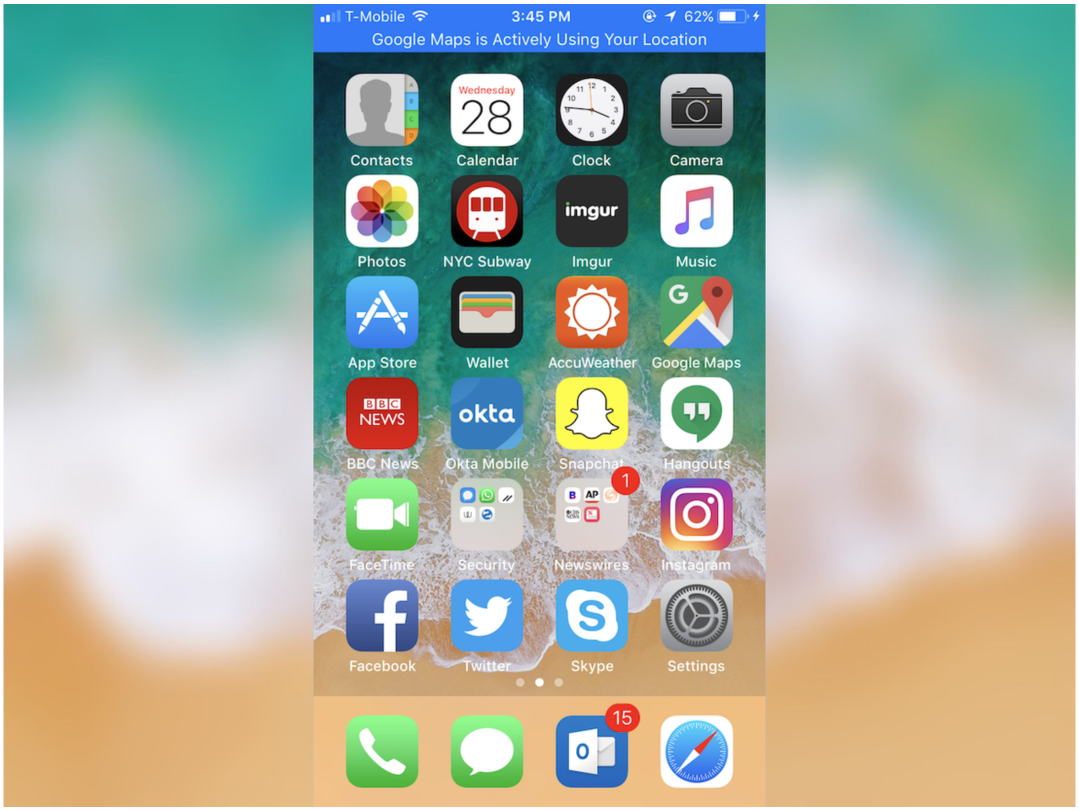
Now, your iOS 11 device gives you more granularity to prevent this kind of constant location tracking.

Go to **Settings > Privacy > Location Services**, then go to any app to check its location permissions. You can now set up the Uber app so that it only collects location data when you're using it -- and no other times.



Use the password manager

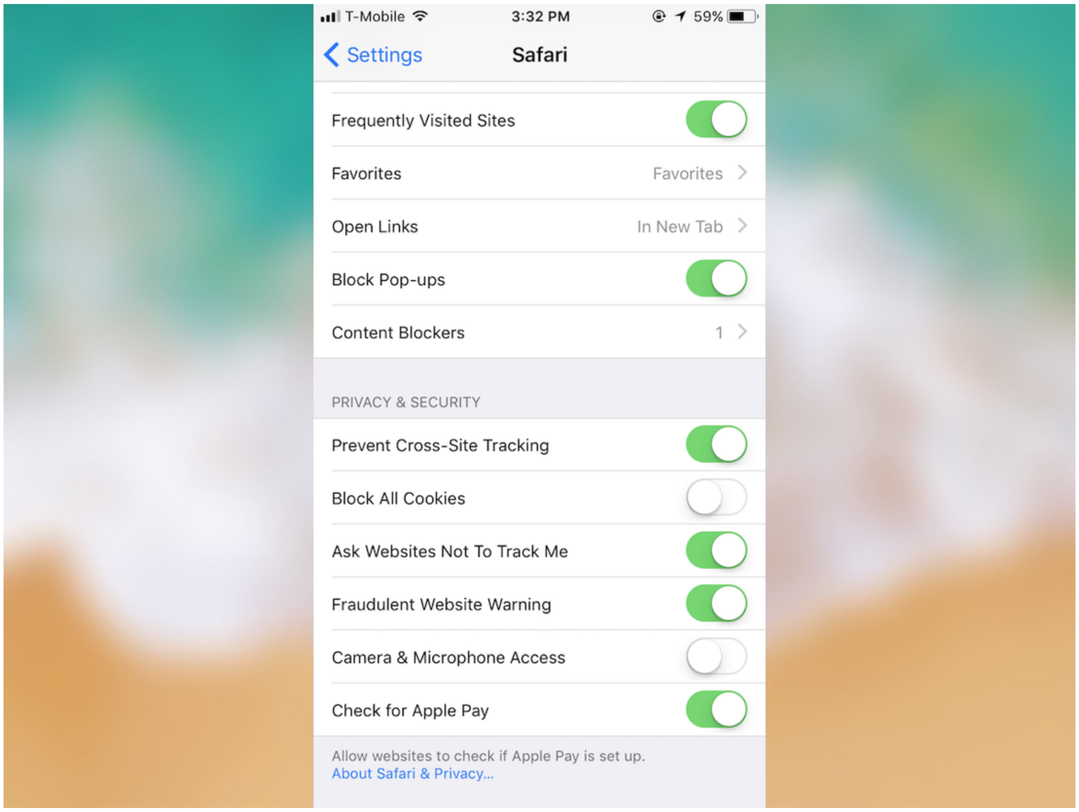
An in-built app friendly password manager might be iOS 11's most underrated feature. With one tap, the login fields are populated with the user's password. The password manager is protected by the user's device passcode, or Touch ID if it's enabled, to prevent others from snooping.



Google Maps is Actively Using Your Location

And watch out for this blue bar...

Apple will now name and shame any app that uses your location outside of the app. Some of these are perfectly benign, like using Google Maps for directions. But if you see this blue bar telling you that an app is looking up where you are, you know to change your app permissions.



T-Mobile 3:32 PM 59%

< Settings Safari

Frequently Visited Sites	☑
Favorites	Favorites >
Open Links	In New Tab >
Block Pop-ups	☑
Content Blockers	1 >

PRIVACY & SECURITY

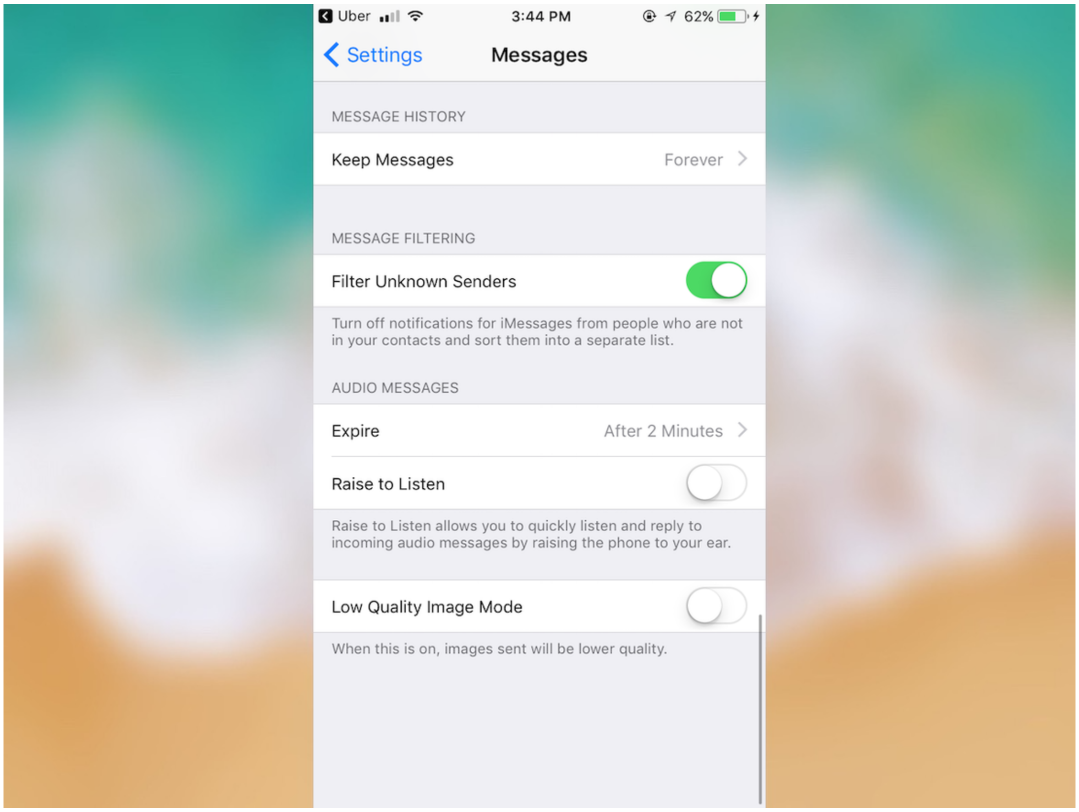
Prevent Cross-Site Tracking	☑
Block All Cookies	☐
Ask Websites Not To Track Me	☑
Fraudulent Website Warning	☑
Camera & Microphone Access	☐
Check for Apple Pay	☑

Allow websites to check if Apple Pay is set up.
About Safari & Privacy...

Change these Safari settings, stat

Safari, your mobile web browser, has several privacy settings worth exploring. Apple now puts new restrictions on how cookies can be used to personalize ads, making it tougher for advertisers to track you across websites. Apple says the intent is to ensure that users only have persistent cookies from sites they interact with while tracking data is continuously cleaned out.

Go to **Settings > Safari** and switch on **Block Pop-ups**, and **prevent Cross-Site Tracking** to stop advertisers from monitoring your browsing habits, and **Ask Websites Not to Track Me** in case they have a setting enabled. You're also safer by using the built-in **Fraudulent Website Warning**, which detects nefarious, phishing pages.



Messages

MESSAGE HISTORY

Keep Messages: Forever

MESSAGE FILTERING

Filter Unknown Senders: on

Turn off notifications for iMessages from people who are not in your contacts and sort them into a separate list.

AUDIO MESSAGES

Expire: After 2 Minutes

Raise to Listen: off

Raise to Listen allows you to quickly listen and reply to incoming audio messages by raising the phone to your ear.

Low Quality Image Mode: off

When this is on, images sent will be lower quality.

Cut down on text message spam

iMessage is end-to-end encrypted, so not even Apple can read your messages. But one way your privacy is threatened is by the data stored on the device itself. The longer you keep them on your device, the greater the risk that those conversations can be read by others.

To reduce the time in which iMessage data is stored on your device, go to **Settings > Messages > Keep Messages**, and select the time you wish to retain your messages. Go back a step and check the **Audio Messages** and **Video Messages** as well. These options offer shorter life-spans.

You should also switch on **Filter Unknown Senders** to cut down on text message spam.

original article:
http://www.zdnet.com/pictures/new-to-ios-11-change-these-privacy-and-security-settings-right-now/16/